Maryland Public and Confidential Information Policy

Last Updated: 01/31/2017

Contents

1.0 Purpose

The establishment of data classification levels is an important part of ensuring the protection and dissemination of potentially confidential data. The Maryland Department of Information Technology (DoIT) is committed to managing the confidentiality, integrity, and availability of information processed, stored, or transmitted by its information technology (IT) networks, systems, and applications (IT Systems). DoIT will utilize the definitions and guidelines as established by the State of Maryland and relevant laws, such as 2013 Maryland Code §§10-1301 – 1308 **(Md. State Govt. Code §§ 10-1301 to -1308**), relating to Public and Confidential Information to classify and protect its information.

2.0 Document and Review History

This policy supersedes the Maryland Information Security Policy v3.1 (2013) Section 3.1: Information Classification Policy and any related policy regarding public and confidential information declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy is applicable to all information that is processed, stored, or transmitted via IT Assets owned or operated by the Executive Branch of the State of Maryland as well as vendors, contractors, individuals, or other entities providing services for, or on behalf of, the Executive Branch of the State of Maryland. Confidential information can include all information and digital content produced, processed, collected, and stored electronically, on paper or other physical media, and shared orally or visually. All employees, contractors, and vendors of IT resources are responsible for adhering to this policy.

4.0 Policy

This policy establishes the requirements for the Maryland Department of Information Technology and affiliated entities to provide due care and due diligence in protecting and disseminating confidential data. This policy identifies what is considered ‘confidential information’ and the measures required to protect this information.

4.1 General

All Maryland State information is categorized into two main classifications with regard to disclosure:

- Public Information
- Confidential (Non-Public) Information
  - Personally Identifiable Information (PII) (see section 4.3.1)
  - Privileged Information (see section 4.3.2)
  - Sensitive Information (see section 4.3.3)

Any Maryland agency that handles federal data may be subject to a different classification schema than the State standard outlined in this policy.

In addition to following Maryland law related to confidential information, IT systems that process, store or transmit other protected types of information such as Protected Health Information (PHI) and payment card information must abide by the relevant regulation and standard (See *HIPAA Security Rule Policy* and *PCI DSS Compliance Policy*).

NOTE: If an employee is uncertain of the classification of a particular piece of information, the employee should contact his or her manager or Federal liaison for further instruction and clarification. Maryland law does not relieve an agency from a duty to comply with other requirements of federal law or private industry standards.

4.2 Public Information

Public information is information that has been declared publicly available by a Maryland State official with the explicit authority to do so, and can be freely given to anyone without concern for potential impact to the State of Maryland, its employees, or citizens.

4.3 Confidential Information

Confidential information is non-public information and is defined by the sub-categories described in the following sections, 4.3.1 – 4.3.3.

4.3.1 Personally Identifiable Information (PII)

PII is defined as data elements such as an individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image combined with one or more of the following:

- A Social Security number;
- a driver's license number, state identification card number, or other individual identification number issued by a unit;
- a passport number or other identification number issued by the United States government;
- an Individual Taxpayer Identification Number; or

- a financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account.

4.3.2 Privileged Information

Privileged information is protected from disclosure by the doctrine of executive privilege, which may include, but is not limited to, records:

- Relating to budgetary and fiscal analyses, policy papers, and recommendations made by the Department or by any person working for the Department
- Provided by any other agency to the Department in the course of the Department's exercise of its responsibility to prepare and monitor the execution of the annual budget
- Relating to a State procurement when a final contract award has not been made or when disclosure of the record would adversely affect future procurement activity
- Of confidential advisory and deliberative communications relating to the preparation of projects conducted by the Department pursuant to State Finance and Procurement Article, §7-103, Annotated Code of Maryland.

4.3.3 Sensitive Information

Sensitive information is information that if divulged could compromise or endanger the citizens or assets of the State.

4.4 Guidelines for Marking and Handling State Owned Information

It is necessary to classify information so every individual that comes in contact with it knows how to properly handle and protect it.

Public Information, which has no restrictions on disclosure, shall be identified and handled according to the requirements shown in the table below.

#	Public Information	Protection Requirement
A	Marking	No marking requirements
B	Access	Unrestricted
C	Distribution within Maryland State System	No restrictions
D	Distribution outside of Maryland State System	No restrictions
E	Storage	Standard operating procedures based on the highest security category of information recorded on the media (See *Security Assessment Policy*)
F	Disposal/Destruction	See *Media Protection Policy* for disposal instructions.
G	Penalty for deliberate or inadvertent disclosure	Not applicable

Confidential information, if disclosed, could result in a negative impact to the State of Maryland, its employees, or citizens and shall be identified and handled according to the requirements shown in the table below.

#	Confidential Information	Protection Requirement
A	Marking	Confidential information is to be clearly identified as 'Confidential'.
B	Access	Access is limited to individuals who have signed a non-disclosure agreement and have been identified as: ▪ Only those Maryland State employees or contractors with explicit **need-to-know**; or ▪ Other individuals for whom an authorized Maryland State official has determined there is a mission-essential **need-to-share**.
C	Distribution within Maryland State System	Delivered direct – signature required, envelopes stamped 'Confidential', or an approved, electronic email or electronic file transmission method.
D	Distribution outside of Maryland State System	Delivered direct – signature required, approved private carriers, or approved encrypted electronic email or encrypted electronic file transmission method.
E	Storage	▪ Control physical access to system media (paper or digital) and protect confidential data using **encryption technologies** or other substantial mitigating controls (such as Data Loss Prevention, Network Security Event Monitoring and strict database change monitoring) ▪ Storage is prohibited on portable devices and publicly accessible systems unless prior written approval from agency Secretary (or delegated authority) has been granted ▪ Approved storage on portable devices or publicly accessible devices must be encrypted ▪ Keep from view by unauthorized individuals, protect against viewing while in use, and when unattended, store in locked desks, cabinets, or offices within a physically secured building.
F	Disposal/Destruction	Dispose of paper information in specially marked disposal bins on Maryland State premises or shred; electronic storage media is sanitized or destroyed using an approved method. See *Media Protection Policy* for further disposal instructions.
G	Penalty for deliberate or inadvertent disclosure	The penalty for deliberate or inadvertent disclosure of confidential information can range from administrative actions to adverse personnel actions up to termination of employment. Deliberate, unauthorized disclosure of confidential information may result in civil and/or criminal penalties.

4.5 Breach Requirements

Breach requirements of Personally Identifiable Information are outlined within 2013 Maryland Code §10-1301. Under the Maryland statute, a breach is considered to be any "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a unit." Additionally, if a unit discovers or is notified of a breach, it must conduct in good faith a reasonable and prompt investigation to determine

whether the unauthorized acquisition of personal information of the individual has resulted in or is likely to result in the misuse of the information.

After an investigation is concluded, the unit must determine if notification is required under the specific circumstances. A unit or nonaffiliated third party is not required to notify an individual of a breach if the personal information of the individual was secured by encryption or redacted and the encryption key has not been compromised or disclosed. See 2013 Maryland Code §§10-1301-1308 for further information on notification requirements.

NOTE: This policy provides guidance for compliance with specific portions of the Maryland Code §§10-1301-1308, but does not supplement, replace or supersede the Maryland law itself. Agencies and associated vendors or contractors of executive agencies are responsible for independently complying with all provisions of Maryland law and other regulations/standards that affect specific types of Confidential Data, such as PHI (covered under the Health Insurance Portability and Accountability Act).

5.0 Exemptions

The requirements of this policy are established by Federal and Maryland laws and standards; there are no exemptions to this policy.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Additional related policies include:

- Asset Management Policy
- Cybersecurity Incident Response Policy and associated processes
- HIPAA Security Rule Policy
- Media Protection Policy
- PCI DSS Compliance Policy
- Security Assessment Policy

7.0 Definitions

Term	Definition
Encryption Technologies	The process of changing plaintext into ciphertext for the purpose of security or privacy. ▪ Encryption technologies used within Maryland must use FIPS 140-2 validated cryptographic modules to authenticate and encrypt managed network communications.
Md. State Govt. Code §§ 10-1301 to -1308	Maryland law pertaining to the protection of personal information by Executive Agencies within Maryland.
Need-to-know	A security principle that confidential information will only be given to people who need it to do a particular job.
Need-to-share	A security principle that Confidential information will only be given to those people whose mission may be affected by the information.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for creating and enforcing policies for agencies under its policy authority. The Enterprise and all Executive Branch agencies will exercise due diligence and due care to protect all confidential data.

Any personnel responsible for the deliberate or inadvertent disclosure of confidential information may, pending the results of an investigation, be held liable and subject to disciplinary action, including written reprimand, suspension, termination, or possibly criminal and/or civil penalties.